Available online at www.sciencedirect.com
SCIENCE DIRECT®
European Journal of Combinatorics 28 (2007) 322–336
European Journal of Combinatorics
www.elsevier.com/locate/ejc

Subsquare-free Latin squares of odd order

Barbara Maenhaut[a], Ian M. Wanless[b,1], Bridget S. Webb[c]

[a] *Department of Mathematics, The University of Queensland, QLD 4072, Australia*
[b] *Department of Computer Science, Australian National University, Canberra ACT 0200, Australia*
[c] *Pure Mathematics Department, The Open University, Milton Keynes, MK7 6AA, United Kingdom*

Received 17 September 2004; accepted 5 July 2005
Available online 22 August 2005

Abstract

For every odd positive integer m we prove the existence of a Latin square of order $3m$ having no proper Latin subsquares. Combining this with previously known results it follows that subsquare-free Latin squares exist for all odd orders.

1. Introduction

A *Latin square of order n* is a matrix of order n in which each one of n symbols appears exactly once in each row and exactly once in each column. In this paper we assume that the symbol set is $\mathbb{Z}_n$ and we use the same set to index the rows and columns. A *subsquare* of a Latin square L is a submatrix of L which is itself a Latin square. A subsquare of L is *proper* if it has order at least 2 and is not L itself. A Latin square with no proper subsquares is said to be N_∞. Around 1970, A.J.W. Hilton conjectured that N_∞ Latin squares exist for all sufficiently large orders. His conjecture seems to have first appeared in print as Problem 1.7 in [2] (although it is stated incorrectly there). A number of people have considered the problem since then but it remains open. See [3, ch. 4] for a survey of results prior to 1991

E-mail addresses: bmm@maths.uq.edu.au (B. Maenhaut), imw@cs.anu.edu.au (I.M. Wanless), b.s.webb@open.ac.uk (B.S. Webb).

[1] Current address: School of Engineering and Logistics, Charles Darwin University, Darwin, NT 0909, Australia.

0195-6698/$ - see front matter
doi:10.1016/j.ejc.2005.07.002

and [5,7] and [8] for subsequent constructions. For an upper bound on the proportion of order n Latin squares which are N_∞, see [6]. Currently the best general existence result for N_∞ squares is due to Andersen and Mendelsohn [1]:

Theorem 1.1. *If n is divisible by a prime ≥ 5 then there exists an N_∞ Latin square of order n.*

The purpose of this paper is to prove:

Theorem 1.2. *If n is odd and divisible by 3 then there exists an N_∞ Latin square of order n.*

Combining the two preceding theorems, we have:

Theorem 1.3. *For all odd n, there exists an N_∞ Latin square of order n.*

The existence of N_∞ Latin squares of large orders of the form $2^a 3^b$ for $a \geq 1$ and $b \geq 0$ remains open. Our construction for proving Theorem 1.2 was originally proposed by Wanless [8].

2. The construction

It is often useful to think of a Latin square of order n as a set of n^2 triples of the form (*row, column, symbol*). The Latin property means that distinct triples never agree in more than one coordinate. For a Latin square L, we say that the triple $(i, j, L_{i,j})$ belongs to L and write $(i, j, L_{i,j}) \in L$. Throughout this paper, the term *entry* refers to a triple and *symbol* refers to the third coordinate of a triple. For each Latin square there are six *conjugate* squares obtained by (uniformly) permuting the coordinates of each triple. For example, the transpose of L is obtained by swapping the row and column coordinates in each triple. The *row-inverse* of L is obtained by swapping the column and symbol coordinates in each triple. This has the effect of replacing each row, when thought of as a permutation, by its inverse permutation.

We define the d-th *diagonal*, denoted as $\mathcal{D}[d]$, of a Latin square L of order n, to be the set of entries (i, j, k) satisfying $j - i \equiv d \mod n$. In particular, $\mathcal{D}[0]$ is the main diagonal. We say that $\mathcal{D}[d]$ of L is *cyclic* if the entries on it occur in cyclic order, that is, $L_{i,i+d} + 1 \equiv L_{i+1,i+1+d}$ for each i, where all calculations are in $\mathbb{Z}_n$. We then define a *diagonally cyclic* Latin square to be a Latin square in which each diagonal is cyclic. A diagonally cyclic Latin square L is generated from its first row by applying the rule that the entry $(i, j, L_{i,j})$ implies the entry $(i + 1, j + 1, L_{i,j} + 1)$, where all additions are in $\mathbb{Z}_n$. In fact, the square can be generated using this rule given any single row or column.

In [8] Wanless gave a survey of applications for diagonally cyclic Latin squares. He also gave a construction for a diagonally cyclic Latin square of each odd order n, which he conjectured might be N_∞. His computer confirmed this conjecture for $n \leq 10\,000$. In this paper we prove a particular case of the conjecture, namely the case when the order is divisible by 3. In this case, the construction can be described as follows. Let $n = 3m$ for

$$\begin{pmatrix}
0 & 4 & 3 & 2 & 1 & 13 & 12 & 11 & 10 & 14 & 8 & 7 & 6 & 5 & 9 \\
10 & 1 & 5 & 4 & 3 & 2 & 14 & 13 & 12 & 11 & 0 & 9 & 8 & 7 & 6 \\
7 & 11 & 2 & 6 & 5 & 4 & 3 & 0 & 14 & 13 & 12 & 1 & 10 & 9 & 8 \\
9 & 8 & 12 & 3 & 7 & 6 & 5 & 4 & 1 & 0 & 14 & 13 & 2 & 11 & 10 \\
11 & 10 & 9 & 13 & 4 & 8 & 7 & 6 & 5 & 2 & 1 & 0 & 14 & 3 & 12 \\
13 & 12 & 11 & 10 & 14 & 5 & 9 & 8 & 7 & 6 & 3 & 2 & 1 & 0 & 4 \\
5 & 14 & 13 & 12 & 11 & 0 & 6 & 10 & 9 & 8 & 7 & 4 & 3 & 2 & 1 \\
2 & 6 & 0 & 14 & 13 & 12 & 1 & 7 & 11 & 10 & 9 & 8 & 5 & 4 & 3 \\
4 & 3 & 7 & 1 & 0 & 14 & 13 & 2 & 8 & 12 & 11 & 10 & 9 & 6 & 5 \\
6 & 5 & 4 & 8 & 2 & 1 & 0 & 14 & 3 & 9 & 13 & 12 & 11 & 10 & 7 \\
8 & 7 & 6 & 5 & 9 & 3 & 2 & 1 & 0 & 4 & 10 & 14 & 13 & 12 & 11 \\
12 & 9 & 8 & 7 & 6 & 10 & 4 & 3 & 2 & 1 & 5 & 11 & 0 & 14 & 13 \\
14 & 13 & 10 & 9 & 8 & 7 & 11 & 5 & 4 & 3 & 2 & 6 & 12 & 1 & 0 \\
1 & 0 & 14 & 11 & 10 & 9 & 8 & 12 & 6 & 5 & 4 & 3 & 7 & 13 & 2 \\
3 & 2 & 1 & 0 & 12 & 11 & 10 & 9 & 13 & 7 & 6 & 5 & 4 & 8 & 14
\end{pmatrix}$$

Fig. 1. The construction for $n = 15$.

an odd integer m. Define the zeroth row of a Latin square L of order n by

$$L_{0,i} = \begin{cases} 0 & \text{if } i = 0, \\ 3m-1 & \text{if } i = 2m-1, \\ 2m-1 & \text{if } i = 3m-1, \\ m-i & \text{if } 1 \le i < m, \\ 4m-2-i & \text{otherwise.} \end{cases} \tag{1}$$

The remaining rows of L are defined by the diagonally cyclic property. Wanless showed that (1) defines a diagonally cyclic Latin square which is equal to its row-inverse. An example of the construction, for the case $m = 5$, is given in Fig. 1.

In the remainder of this paper, the following notation will be fixed. Firstly, $n = 3m$ for an odd positive integer m. Secondly, L will be the diagonally cyclic Latin square of order n defined by (1). Thirdly, S will be a proper N_∞ subsquare of L of order s (our goal is to prove the non-existence of S, which then implies the non-existence of any proper subsquares in L). All row and column indices will refer to L rather than to S. Furthermore, let π be the map which applies the permutation $x \mapsto x + 1 \bmod n$ to each of the three coordinates in the triples of L. Although we have defined π as acting on all the triples of L we also use it to denote the induced action on any subset of the triples of L. Since L is diagonally cyclic, π is an automorphism of L, meaning that the set of triples in L is invariant (as a set) under the application of π. This observation will prove extremely useful in subsequent sections. Finally, let τ be the map acting on the triples of L according to the rule $(i, j, k) \mapsto (i, k, j)$. Note that τ is well defined since L is equal to its row-inverse.

We also need some terminology to describe parts of L. We say that L has six *regions*. Each region consists of either a single diagonal or $m - 1$ consecutive diagonals.

- Region 0 is $\mathcal{D}[0]$.
- Region 1 is $\mathcal{D}[1] \cup \mathcal{D}[2] \cup \cdots \cup \mathcal{D}[m-1]$.

- Region 2 is $\mathcal{D}[m] \cup \mathcal{D}[m+1] \cup \cdots \cup \mathcal{D}[2m-2]$.
- Region 3 is $\mathcal{D}[2m-1]$.
- Region 4 is $\mathcal{D}[2m] \cup \mathcal{D}[2m+1] \cup \cdots \cup \mathcal{D}[3m-2]$.
- Region 5 is $\mathcal{D}[3m-1]$.

Diagonals $\mathcal{D}[0]$, $\mathcal{D}[1]$, $\mathcal{D}[m]$, $\mathcal{D}[2m-1]$, $\mathcal{D}[2m]$, $\mathcal{D}[3m-1]$ are the *principal diagonals*, and diagonals $\mathcal{D}[0]$, $\mathcal{D}[2m-1]$ and $\mathcal{D}[3m-1]$ (that is, regions 0, 3 and 5) are called *special diagonals*. Note that within each region, the symbol directly to the right of x is $x-1$. Furthermore, for a region i, let $\sigma(i)$ be the symbol in row zero of the principal diagonal of region i, and let $\delta(i)$ be the index of the principal diagonal of region i. Thus

$$\begin{aligned}
\sigma(0) &= 0, & \delta(0) &= 0,\\
\sigma(1) &= m-1, & \delta(1) &= 1,\\
\sigma(2) &= 3m-2, & \delta(2) &= m,\\
\sigma(3) &= 3m-1, & \delta(3) &= 2m-1,\\
\sigma(4) &= 2m-2, & \delta(4) &= 2m,\\
\sigma(5) &= 2m-1, & \delta(5) &= 3m-1.
\end{aligned}$$

3. Algorithm for locating short cycles

In this section we describe the algorithm that was used to locate short row cycles in L. The results of this algorithm will be presented in the next section, where they will be used to show that L has no small subsquares.

By a *subrectangle* of L we mean a rectangular submatrix of L in which the same symbols occur in each row. If R is a $2 \times \ell$ subrectangle of L, and R is minimal in that it contains no $2 \times \ell'$ subrectangle for $2 \le \ell' < \ell$, then we say that R is a *row cycle* of length ℓ. Note that a row cycle of length ℓ between two rows r and r' corresponds in a natural way to a cycle of length ℓ in the permutation which maps $L_{r,x} \mapsto L_{r',x}$ for each column x. In what follows the term *cycle* should be understood to mean a row cycle of L.

In searching for short cycles, we use the symmetries of L to reduce the search space, by developing a notion of equivalence for subrectangles. The concept will later be applied to two different types of subrectangle, namely cycles and (hypothetical) subsquares.

We impose a partial order called *importance* on the six regions of L. There are three levels of importance, with the region of greatest importance being region 0. The other two special diagonals (regions 3 and 5) are of intermediate importance and the remaining three regions are of lowest importance. Each entry of L is deemed to have the same level of importance as the region it inhabits.

We say that a subrectangle R is *well-placed* if it contains an entry, called the *root*, having particular properties. The defining properties of the root are that it is in row 0, on a principal diagonal other than $\mathcal{D}[3m-1]$, and is at least as important as any other entry of R. From the first part of the definition we know that the root is always one of the following five entries of L:

$$(0,0,0),\ (0,1,m-1),\ (0,m,3m-2),\ (0,2m-1,3m-1),\ (0,2m,2m-2). \quad (2)$$

Moreover, the root must be $(0, 0, 0)$ if R includes any entry on the main diagonal and must be either $(0, 0, 0)$ or $(0, 2m - 1, 3m - 1)$ if any entry of R lies on a special diagonal. One crucial property of well-placed subrectangles follows straight from the definition. If R is well-placed then every cycle of R which includes the root is itself a well-placed subrectangle, using the same root.

Next, we introduce $\mathcal{L}$, the *left shift operator*, which maps each entry $(x, y, L_{x,y})$ to the entry on its left, namely $(x, y - 1, L_{x,y-1})$. If (x, y, z) is not on a principal diagonal then $\mathcal{L}((x, y, z)) = (x, y - 1, z + 1)$. It follows that if a subrectangle R contains no entry on a principal diagonal then applying $\mathcal{L}$ to the entries of R produces another subrectangle, which we denote as $\mathcal{L}(R)$.

We consider two subrectangles to be *equivalent* if one can be mapped to the other by some sequence of applications of π, τ and $\mathcal{L}$. This equivalence partitions the set of subrectangles into equivalence classes and each of these classes contains at least one well-placed representative. We now give a constructive proof of this last fact.

Consider a general subrectangle R. Firstly, if R contains no entry on a principal diagonal we replace R by $\mathcal{L}(R)$. After repeated application of this rule we must find an R which contains an entry on a principal diagonal. Secondly, if the only entries on special diagonals in R lie in region 5 then we replace R by its image under τ, so then R contains an entry in region 3. Thirdly, by repeated replacement of R with its image under the automorphism π we can "slide" any given entry down its diagonal until it lies in row 0 on the same diagonal. We choose to do this to one of the entries on a principal diagonal in R, taking an entry in region 0 by preference, an entry in region 3 as second choice, or failing both those options, any other entry on a principal diagonal. It is easy to check that the chosen entry will be at least as important as any other entry in R and hence will satisfy the criteria for the root.

We can now describe our algorithm, which looks for all well-placed cycles of a given length c between row 0 and row r, where r is a variable that is allowed to take any non-zero value in $\mathbb{Z}_n$. The algorithm works by allocating a region to each entry in a supposed well-placed cycle. It then does some calculations on the basis of these allocations and discovers either an actual cycle or, more often, that the assumed structure forces at least one of the entries to lie outside its designated region. Taking this approach for all possible designations of entries to regions ensures that we find all well-placed cycles of length c.

Luckily, our method only requires us to perform elementary arithmetic operations with our variables. As a result, all calculations can be expressed in terms of linear polynomials in a variable k with the answer being reduced modulo n (which is itself a linear polynomial in k). Crucially, this scheme allows us to solve the problem for a general value of n. It turns out that some small values of n need to be treated as special cases, but we will say more about that later.

We choose as a starting point for our well-placed cycle an entry e_0, in row 0, to be the root. Thus e_0 must be one of the five entries given in (2). The choice of e_0 sometimes places restrictions on other entries of the cycle, given that no other entry of the cycle can have greater importance than e_0.

Having chosen e_0, for $i \in \mathbb{Z}_c$ we define f_i to be the entry in row r in the same column as e_i, and define e_{i-1} to be the entry in row 0 which contains the same symbol as f_i. We designate that e_i belongs to $\mathcal{D}[\delta(t_i) + u_i]$ in region t_i while f_i belongs to $\mathcal{D}[\delta(b_i) + v_i]$ in

```
(A1)  For each m ∈ {2ck + 1, 2ck + 3, 2ck + 5, ..., 2ck + 2c − 1} do
(A2)      n := 3m
(A3)      For each t_0, T = {t_1, t_2, ..., t_{c−1}} and B = {b_0, b_1, ..., b_{c−1}} do
(A4)          Find all non-zero solutions to Eq. (5)
(A5)          If there are any
(A6)              Compute all permutations of T and B
(A7)              For each ordering of T and ordering of B do
(A8)                  For each solution ρ found in step (A4) do
(A9)                      u_0 := 0
(A10)                     valid := true
(A11)                     For i in Z_c while valid do
(A12)                         j := i + 1 mod c
(A13)                         v_j := ρ + u_i + σ(b_j) − σ(t_i)
(A14)                         u_j := ρ + v_j + δ(b_j) − δ(t_j)
(A15)                         Update valid
(A16)                     If valid
(A17)                         Report details of cycle found
```

Fig. 2. Algorithm for finding cycles of length c.

region b_i. In other words,

$$e_i = (0, \delta(t_i) + u_i, \sigma(t_i) - u_i) \qquad \text{and}$$
$$f_i = (r, \delta(b_i) + v_i + r, \sigma(b_i) - v_i + r).$$

We can now write down equations expressing the relationships between the entries in the cycle. For each $i \in \mathbb{Z}_c$, the fact that e_i is in the same column as f_i says that

$$\delta(t_i) + u_i \equiv \delta(b_i) + v_i + r \bmod n, \tag{3}$$

while from the fact that e_i has the same symbol as f_j (where $j = i + 1 \bmod c$) we find that

$$\sigma(t_i) - u_i \equiv \sigma(b_j) - v_j + r \bmod n. \tag{4}$$

Making r the subject of each of these congruences and summing them gives

$$2cr \equiv \sum_{i \in \mathbb{Z}_c} (\delta(t_i) - \delta(b_i) + \sigma(t_i) - \sigma(b_i)) \bmod n. \tag{5}$$

Notice that the u_i and v_i variables have cancelled, so that we can easily solve Eq. (5) for r in terms of k. Since the root must lie on a principal diagonal we know that $u_0 = 0$. Knowing r as well means we can easily find each u_i and v_i from Eqs. (3) and (4).

Fig. 2 gives the algorithm in pseudo-code. We will now offer some explanatory notes in which all step numbers refer to that figure.

In step (A1) we introduce a loop which ensures that m takes every possible odd value modulo $2c$. These c cases are treated separately to facilitate step (A4). The value of m is used in step (A2) to calculate n.

```
if b_2 is divisible by c but b_1 is not then
    there are no solutions
else
    numsols := gcd(b_2, c)
    while b_1 is not divisible by 2c do
        a_1 := a_1 + a_2
        b_1 := b_1 + b_2
    a_1 := a_1/(2c)
    b_1 := b_1/(2c)
    report that a_1 k + b_1 is a solution
    for i from 2 to numsols do
        a_1 := a_1 + a_2/c
        b_1 := b_1 + b_2/c
        report that a_1 k + b_1 is a solution
```

Fig. 3. Algorithm for finding solutions to Eq. (6).

Step (A3) begins the allocation of entries to regions. We do not, at this stage, decide exactly to which region each entry belongs, because Eq. (5) does not depend on the order of the t_i's or the b_i's. Hence it is more efficient to decide on the multiset $\{t_0, t_1, \ldots, t_{c-1}\}$ and the multiset $\{b_0, b_1, \ldots, b_{c-1}\}$ before solving Eq. (5). Only then (if there are any viable solutions) do we need to decide on the ordering which allocates the elements of these multisets to the t_i's and b_i's. In practice, the situation is complicated by the special role played by e_0. Hence in step (A3) we decide to which region e_0 belongs, but for the other entries we simply decide the multisets $T = \{t_1, t_2 \ldots, t_{c-1}\}$ and $B = \{b_0, b_1, \ldots, b_{c-1}\}$.

In step (A4) we solve Eq. (5), which requires us to perform division. Our task is to solve a congruence of the form

$$2cr \equiv a_1 k + b_1 \bmod n \tag{6}$$

where $n = a_2 k + b_2$ and a_1, b_1, a_2, b_2 are integers whose values we know. From step (A1) we know that $m = 2ck + b_3$ for an odd integer b_3. It then follows from Eq. (5) and the definitions of n, $\sigma()$ and $\delta()$ that $2c$ divides both a_2 and a_1. We also know that both b_2 and b_3 are odd. It transpires that we can restrict attention to the case when c is either prime or a power of 2. Under these conditions, the elementary theory of linear congruences justifies the algorithm given in Fig. 3 for finding all solutions to Eq. (6). Every division performed in that algorithm produces a quotient which is an integer.

For many choices of t_0, T and B, there is either no solution to Eq. (5) or there is the unique solution $r = 0$. In either case we need go no further with these choices of t_0, T and B. However, for those choices of t_0, T and B for which there are non-zero solutions to Eq. (5), we need to allocate the t_i's and b_i's, so in step (A6) we compute and store each of the possible permutations of T and B. In step (A7) we begin the loops which work through the possible allocations. In steps (A9) to (A15) we work through the solutions to Eqs. (3) and (4) for each possible allocation and for each possible solution to (5). Given that we know the values of u_0 and r, it is easy to solve Eqs. (4) and (3) by the direct substitutions in steps (A13) and (A14), respectively.

Step (A15) involves checking that the v_j and u_j calculated in steps (A13) and (A14) actually lie in their required range. The required range is $[0, w]$ where $w = 0$ for special diagonals and $w = m - 2$ for other regions. Testing the validity of a variable requires a subroutine to evaluate inequalities between linear polynomials in k, or equivalently, to compare a linear polynomial $ak + b$ with zero. This latter feat is accomplished by looking first at the sign of a and then, if $a = 0$, by looking at the sign of b. This allows the subroutine to decide the behaviour of $ak + b$ for large k. However, the subroutine also keeps track of whether there are any exceptions for small k. So, for example, if asked to evaluate $4k - 9$ the subroutine would return that this is positive, but would note that its conclusion is invalid for $k \leq 2$. The issue of how these small exceptions are handled will be discussed in the next section.

A useful check that the program is working is to check at step (A16) that u_0 is still zero. The value of u_0 is recalculated in the last iteration of the for loop in steps (A9) to (A15), and if ρ was indeed a solution to Eq. (5) then the new u_0 should match the original value. Our program never failed this test.

Of course, if "valid" is still true by step (A16) then each u_i and v_i lies within its allocated range and hence we have found an actual cycle of length c. If "valid" is false then the present allocation of entries to regions is inconsistent with the structure of L, so we proceed to the next case.

In this manner we checked all feasible allocations of entries to regions and found all well-placed row cycles of length c, for $c \in \{2, 3, 4, 5, 7, 8\}$. These results will be given in the next section.

4. No small subsquares

In this section we present the results of the algorithm described in the previous section and then use them to prove that L has no small subsquares.

We list the cycles found by our program, categorized by the cycle length and value of n. Within each of these categories the cycles will be listed according to r, the second row of the cycle (the first row is always row 0).

A cycle of length c will be written as $C_c\{a_1, a_2, \ldots, a_c\}$ where the a_i are the columns involved in the cycle. Hence each a_i is equal to $\delta(t_j) + u_j$ for some j. We have sorted the columns numerically to facilitate comparison between different cycles. The root e_0 occurs in the column which we have written in bold. Of course, all column numbers as well as values of n and r are linear polynomials in the variable k.

Cycles of length 2

Neither case $n = 12k + 3$ nor case $n = 12k + 9$ reported any 2-cycle.

Cycles of length 3

Case: $n = 18k + 3$

$$\begin{aligned} r = 6k + 1 \quad & C_3\{\mathbf{0}, 6k + 1, 18k + 1\} \\ & C_3\{2, 6k + 3, \mathbf{12k + 2}\} \\ & C_3\{6k, \mathbf{12k + 1}, 18k\} \end{aligned}$$

$r = 12k + 2$ $C_3\{\mathbf{0}, 12k, 12k + 2\}$
$C_3\{1, \mathbf{12k + 1}, 12k + 3\}$
$C_3\{2, \mathbf{6k + 1}, 12k + 4\}$

Case: $n = 18k + 9$

$r = 4k + 2$ $C_3\{4k + 3, \mathbf{12k + 5}, 14k + 6\}$
$r = 6k + 3$ $C_3\{\mathbf{0}, 6k + 3, 18k + 7\}$
$C_3\{2, 6k + 5, \mathbf{12k + 6}\}$
$C_3\{6k + 2, \mathbf{12k + 5}, 18k + 6\}$
$r = 12k + 6$ $C_3\{\mathbf{0}, 12k + 4, 12k + 6\}$
$C_3\{1, \mathbf{12k + 5}, 12k + 7\}$
$C_3\{2, \mathbf{6k + 3}, 12k + 8\}$

Case: $n = 18k + 15$

$r = 6k + 5$ $C_3\{\mathbf{0}, 6k + 5, 18k + 13\}$
$C_3\{2, 6k + 7, \mathbf{12k + 10}\}$
$C_3\{6k + 4, \mathbf{12k + 9}, 18k + 12\}$
$r = 10k + 8$ $C_3\{8k + 5, 10k + 6, \mathbf{12k + 9}\}$
$r = 12k + 10$ $C_3\{\mathbf{0}, 12k + 8, 12k + 10\}$
$C_3\{1, \mathbf{12k + 9}, 12k + 11\}$
$C_3\{2, \mathbf{6k + 5}, 12k + 12\}$

Cycles of length 4

None of the cases $n = 24k + 3$, $n = 24k + 9$, $n = 24k + 15$ or $n = 24k + 21$ have any 4-cycles.

Cycles of length 5

Case: $n = 30k + 3$

$r = 6k + 1$ $C_5\{\mathbf{0}, 4k, 6k + 1, 18k + 1, 22k + 1\}$
$r = 12k + 1$ $C_5\{4k, \mathbf{10k + 1}, 16k + 2, 22k + 1, 28k\}$
$r = 18k + 2$ $C_5\{\mathbf{1}, 6k, 12k - 1, 18k, 24k + 3\}$
$r = 24k + 2$ $C_5\{\mathbf{0}, 12k, 16k, 24k + 2, 28k + 2\}$

Case: $n = 30k + 9$

$r = 12k + 4$ $C_5\{\mathbf{0}, 4k, 6k + 3, 12k + 4, 28k + 6\}$
$r = 18k + 5$ $C_5\{\mathbf{0}, 16k + 2, 18k + 5, 22k + 5, 24k + 8\}$

Case: $n = 30k + 15$

$r = 6k + 3$ $C_5\{\mathbf{1}, 6k + 6, 12k + 7, 18k + 10, 24k + 13\}$
$C_5\{2k + 1, 8k + 6, 14k + 7, \mathbf{20k + 10}, 26k + 13\}$

$r = 12k + 6$ $C_5\{\mathbf{1}, 6k + 6, 12k + 9, 18k + 10, 24k + 11\}$
$C_5\{2k + 1, 8k + 6, 14k + 9, \mathbf{20k} + \mathbf{10}, 26k + 11\}$
$r = 18k + 9$ $C_5\{2k + 3, 8k + 4, 14k + 5, \mathbf{20k} + \mathbf{10}, 26k + 15\}$
$C_5\{4k + 4, \mathbf{10k} + \mathbf{5}, 16k + 8, 22k + 13, 28k + 16\}$
$r = 22k + 11$ $C_5\{6k + 4, 8k + 5, \mathbf{20k} + \mathbf{9}, 22k + 12, 24k + 13\}$
$r = 24k + 12$ $C_5\{2k + 3, 8k + 4, 14k + 7, \mathbf{20k} + \mathbf{10}, 26k + 13\}$
$C_5\{4k + 4, \mathbf{10k} + \mathbf{5}, 16k + 10, 22k + 11, 28k + 16\}$

Case: $n = 30k + 21$

$r = 6k + 4$ $C_5\{4k + 2, \mathbf{10k} + \mathbf{7}, 16k + 10, 22k + 15, 28k + 18\}$
$r = 24k + 17$ $C_5\{\mathbf{1}, 6k + 4, 12k + 7, 18k + 12, 24k + 15\}$

Case: $n = 30k + 27$

$r = 16k + 14$ $C_5\{12k + 9, 14k + 10, 16k + 11, 18k + 14, \mathbf{20k} + \mathbf{17}\}$

Cycles of length 6

We did not look for cycles of length 6 since they are not needed for our argument and solving Eq. (5) is harder when c is properly divisible by 3.

Cycles of length 7

The cases $n = 42k + 3$, $n = 42k + 9$ and $n = 42k + 27$ reported no 7-cycles.

Case: $n = 42k + 15$

$r = 18k + 7$ $C_7\{\mathbf{0}, 2k - 1, 6k + 3, 8k + 2, 12k + 6, 18k + 7, 38k + 11\}$
$r = 24k + 8$ $C_7\{\mathbf{0}, 20k + 4, 24k + 8, 26k + 7, 30k + 11, 32k + 10, 36k + 14\}$

Case: $n = 42k + 21$

$r = 4k + 2$
$C_7\{4k + 3, 12k + 7, 20k + 9, 22k + 10, \mathbf{28k} + \mathbf{13}, 30k + 14, 38k + 18\}$
$r = 6k + 3$
$C_7\{\mathbf{0}, 6k + 3, 8k + 4, 18k + 9, 26k + 11, 30k + 15, 38k + 17\}$
$C_7\{\mathbf{1}, 6k + 4, 12k + 7, 18k + 10, 24k + 11, 30k + 16, 36k + 17\}$
$C_7\{2k + 1, 8k + 6, \mathbf{14k} + \mathbf{7}, 20k + 10, 26k + 13, 32k + 16, 38k + 19\}$
$C_7\{4k + 1, 8k + 5, 16k + 7, 26k + 12, \mathbf{28k} + \mathbf{13}, 34k + 16, 38k + 18\}$
$C_7\{4k + 2, 10k + 7, 16k + 8, 22k + 11, \mathbf{28k} + \mathbf{14}, 34k + 17, 40k + 20\}$
$r = 12k + 6$
$C_7\{\mathbf{0}, 2k + 1, 12k + 6, 18k + 9, 20k + 10, 36k + 16, 38k + 17\}$
$C_7\{\mathbf{1}, 6k + 4, 12k + 7, 18k + 10, 24k + 13, 30k + 14, 36k + 17\}$
$C_7\{2k + 2, 4k + 3, 20k + 11, 22k + 12, \mathbf{28k} + \mathbf{13}, 38k + 18, 40k + 19\}$
$C_7\{2k + 3, 8k + 4, \mathbf{14k} + \mathbf{7}, 20k + 12, 26k + 13, 32k + 14, 38k + 19\}$

$C_7\{4k+4, 10k+5, 16k+8, 22k+13, \mathbf{28k+14}, 34k+15, 40k+20\}$

$r = 18k+9$

$C_7\{\mathbf{1}, 6k+6, 12k+11, 18k+14, 24k+15, 30k+16, 36k+17\}$

$C_7\{4k+2, 10k+7, 16k+10, 22k+13, \mathbf{28k+14}, 34k+15, 40k+18\}$

$r = 24k+12$

$C_7\{2k+5, 8k+6, \mathbf{14k+7}, 20k+10, 26k+15, 32k+20, 38k+23\}$

$C_7\{4k+4, 10k+5, 16k+6, 22k+9, \mathbf{28k+14}, 34k+19, 40k+22\}$

$r = 30k+15$

$C_7\{\mathbf{0}, 6k+3, 8k+4, 24k+10, 26k+11, 32k+16, 30k+15\}$

$C_7\{\mathbf{1}, 6k+4, 12k+7, 18k+8, 24k+11, 30k+16, 36k+19\}$

$C_7\{2k+1, 8k+6, \mathbf{14k+7}, 20k+8, 26k+13, 32k+18, 38k+19\}$

$C_7\{4k+2, 10k+7, 16k+8, 22k+9, \mathbf{28k+14}, 34k+19, 40k+20\}$

$C_7\{8k+5, 10k+6, 16k+7, 26k+12, \mathbf{28k+13}, 32k+17, 34k+18\}$

$r = 36k+18$

$C_7\{\mathbf{0}, 2k+1, 12k+6, 20k+8, 24k+12, 32k+14, 36k+18\}$

$C_7\{\mathbf{1}, 6k+4, 12k+7, 18k+8, 24k+13, 30k+14, 36k+19\}$

$C_7\{2k+2, 10k+4, 20k+9, 22k+10, \mathbf{28k+13}, 32k+15, 40k+19\}$

$C_7\{2k+3, 8k+4, \mathbf{14k+7}, 20k+10, 26k+13, 32k+16, 38k+19\}$

$C_7\{4k+4, 10k+5, 16k+8, 22k+11, \mathbf{28k+14}, 34k+17, 40k+20\}$

Case: $n = 42k+33$

$r = 10k+8$

$C_7\{8k+7, 10k+10, 12k+11, \mathbf{28k+21}, 30k+24, 32k+25, 34k+26\}$

$r = 18k+14$

$C_7\{2k-1, 8k+6, \mathbf{14k+11}, 20k+16, 26k+19, 32k+22, 38k+25\}$

$r = 24k+19$

$C_7\{\mathbf{1}, 6k+4, 12k+7, 18k+10, 24k+15, 30k+22, 36k+29\}$

Case: $n = 42k+39$

$r = 22k+20$

$C_7\{16k+13, 18k+14, 20k+15, 22k+16, 24k+19, 26k+22, \mathbf{28k+25}\}$

Cycles of length 8

The cases $n = 48k+3$, $n = 48k+9$, $n = 48k+21$, $n = 48k+27$, $n = 48k+33$, and $n = 48k+45$ reported no 8-cycles.

Case: $n = 48k+15$

$r = 22k+7$

$C_8\{4k-3, 8k, 12k+3, \mathbf{32k+9}, 36k+8, 40k+7, 44k+8, 48k+9\}$

Case: $n = 48k + 39$

$r = 22k + 18$

$C_8\{4k - 1, 8k + 4, 12k + 9, \mathbf{32k + 25}, 36k + 26, 40k + 27, 44k + 30, 48k + 33\}$.

As mentioned in the previous section, each time the program tested an inequality there was a possibility that the overall behaviour would have a few small exceptions. The program did all calculations assuming that k is large, but also kept track of K, the largest value of k for which at least one inequality would not follow the general rule. The largest value of K returned by any run of the program was $K = 2$ (for the shorter cycles the value was typically 0 or 1). Hence all of the information on cycles reported above is reliable, so long as we assume that $n > 48 \times 2 + 45 = 141$. The exclusion of small values of n presents no problem since L is known [8] to be N_∞ for all $n < 10\,000$.

The special treatment of small values of n is required for two reasons. Firstly, for a small value of n, the general cycles listed above may not occur. For example, consider the cycle

$C_7\{\mathbf{1}, 6k + 6, 12k + 11, 18k + 14, 24k + 15, 30k + 16, 36k + 17\}$

involving row $r = 18k + 9$, reported above in the case $n = 42k + 21$. This cycle does not exist when $k \leq 2$ since in that case $12k + 11 \geq 14k + 7 = m$, so that the entry in row 0, column $12k + 11$ lies in region 2 rather than region 1. Secondly, there are cycles not listed above which do occur when k is small. For example, our program reported no 4-cycles for $k > 1$, but the example in Fig. 1 (for which $k = 0$) has a 4-cycle between row 0 and row 6, involving the columns 1, 9, 10 and 11.

Having located all the well-placed short cycles (assuming n is moderately large) we are now in a position to argue that there are no small subsquares in L.

Theorem 4.1. *L has no proper subsquares of order* 8 *or less.*

Proof. Suppose that S is a subsquare of order $s \leq 8$. Without loss of generality we can insist that S is an N_∞ subsquare and that S is well-placed. We suppose that S intersects rows $0, r_1, r_2, \ldots r_{s-1}$ and we use γ_i to denote the cycle between row 0 and row r_i which contains the root e_0. Hence, as discussed in the previous section, every cycle γ_i is also well-placed and must occur in the list provided above. It is now a matter of systematically looking through that list to rule out the existence of S.

Subsquares of order 2 (*intercalates*): There are no intercalates because an intercalate is simply a 2-cycle and the program found no 2-cycles.

Subsquares of order 3: The cycles γ_1 and γ_2 must both appear (within the same case) among the cycles of length 3 listed above. Furthermore, they must be located within the same columns. A quick scan of the list shows that no pair of cycles fits these conditions.

Subsquares of order 4: S cannot have order 4 since there are no N_∞ Latin squares of order 4.

Subsquares of order 5: Since the only N_∞ squares of order 5 belong to the main class of the cyclic group table, this case is very much like the case $s = 3$ above. We need cycles $\gamma_1, \gamma_2, \gamma_3$ and γ_4 from within the same case among the cycles of length 5 listed above.

These four cycles must involve the same columns, but the list does not even contain a pair of cycles which use the same columns.

Subsquares of order 6: S cannot have order 6 since there are no N_∞ Latin squares of order 6.

Subsquares of order 7: Our program ruled out all cycles of length 2 or 4. The only partition of 7 which contains no part equal to 1, 2 or 4 is the trivial partition consisting of a single part. From this information we conclude that each γ_i must be a cycle of length 7, so this case works like the cases $s = 3$ and $s = 5$ above.

Subsquares of order 8: Here there are 14 isotopy classes of N_∞ squares to consider, as shown by Denniston [4]. It can be checked that every row in each of the squares in these 14 classes is contained in at least two cycles of length 8. Since our program showed that there is at most one well-placed cycle of length 8 for any given value of n, this means that S cannot have order 8. □

5. No large subsquares

By Theorem 4.1, if S exists then it has order $s \geq 9$. The aim of this section is to demonstrate that such a proper subsquare cannot exist, thereby proving Theorem 1.2.

Throughout this section d will denote the minimum gap between two rows of S. That is, there exist two rows of S with indices, say, r and $r+d \pmod n$, but there do not exist rows with indices r' and $r'+d' \pmod n$ where $0 < d' < d$. Given that π is an automorphism of L, we lose no generality by assuming that S contains rows 0 and d. We define a subset T of $\mathbb{Z}_n$ to be *t-regular* if t divides n and T is a coset of the unique subgroup of index t in $\mathbb{Z}_n$.

If the rows of S are d-regular, then we conclude that d divides n, the set of rows intersecting S must be $\{0, d, 2d, \ldots, n-d\}$ and $s = n/d$. Note that since $s \geq 9$, we have $d \leq \frac{1}{9}n = \frac{1}{3}m$.

Lemma 5.1. *The rows of S are not d-regular.*

Proof. Assume that the rows of S are d-regular. We first argue that this implies that the columns of S are also d-regular.

Let x be an arbitrary column intersecting S. Define $i \geq 1$ to be as small as possible subject to the condition that $\mathcal{D}[i]$ intersects S in column x. Since S is d-regular we know that $1 \leq i \leq d$. Let a be the symbol at the intersection of $\mathcal{D}[i]$ and column x, so that $(x-i, x, a) \in S$. As S is d-regular, S intersects row $x-i+d$. Since $1 \leq i \leq d$ we know that $i+d \leq m-1$, so both $\mathcal{D}[i]$ and $\mathcal{D}[i+d]$ are in region 1. Hence, the symbol a occurs in column $x+2d$ of row $x-i+d$, which means that $(x-i+d, x+2d, a) \in S$.

We apply the above argument starting with column $x+2d$ and conclude that column $x+4d$ intersects S. Continuing in this manner, we deduce that the set of columns intersecting S is $\{x, x+2d, x+4d, \ldots, x+d, x+3d, \ldots\}$, and thus the columns of S are d-regular. It follows from the d-regularity of both rows and columns that $S = \pi^d(S)$.

Since $s \geq 9$, there must be columns $x \in [1, m-1]$ and $y \in [m, 2m-2]$ and symbols a, b such that $(0, x, a) \in S$ and $(0, y, b) \in S$. Now $y - x = \mu d$, for some integer μ. Also

$a = m - x$ and $b = 4m - 2 - y$ so that

$$a - b = (m - x) - (4m - 2 - y) \equiv y - x + 2 = \mu d + 2 \bmod n.$$

Starting with the entry $(0, x, a)$ and repeatedly applying π^d, we find n/d distinct symbols in S (which therefore comprises the entire symbol set of S). These are given by $\{a + \lambda d : \lambda \in \mathbb{Z}\}$. However, by the same argument starting with $(0, y, b)$ we see that the symbol set of S is

$$\{b + \lambda d : \lambda \in \mathbb{Z}\} = \{a + \lambda d - 2 : \lambda \in \mathbb{Z}\}.$$

Hence, if ω is a symbol in S, then so is $\omega - 2$. Thus all symbols must occur in S, and S is not proper, giving the required contradiction. □

A concept that will be useful in the remainder of the paper is that of a *diagonal pair*, by which we mean a pair of entries at distance $2d$ apart on the same diagonal. In other words, the first entry of the diagonal pair is mapped to the second by π^{2d}.

Lemma 5.2. *The subsquare S does not contain two distinct diagonal pairs.*

Proof. Suppose that S contains the following four entries:

$$(r_a, c_a, a),\ (r_a + 2d, c_a + 2d, a + 2d),\ (r_b, c_b, b),\ (r_b + 2d, c_b + 2d, b + 2d),$$

where $(r_a, c_a, a) \neq (r_b, c_b, b)$. If we apply π^{2d} to S then the image $\pi^{2d}(S)$, another subsquare of L, includes two of the entries from S, namely:

$$(r_a + 2d, c_a + 2d, a + 2d), \text{ and } (r_b + 2d, c_b + 2d, b + 2d).$$

It is well known that in any Latin square, if two subsquares intersect, then their intersection is itself a subsquare. As S is assumed to be N_∞, its only subsquare with more than one entry is itself. We conclude that $S = \pi^{2d}(S)$. Since π has order n and n is odd, it follows that $S = \pi^{2d(n+1)/2}(S) = \pi^{dn+d}(S) = \pi^d(S)$. However, if S is invariant under π^d and d is the minimum row gap, it follows that the rows of S are d-regular, contradicting Lemma 5.1. □

We are at last ready to prove our main result.

Proof of Theorem 1.2. By Theorem 4.1, we may assume that $s \geq 9$. Also, as above, we assume that S intersects rows 0 and d where d is the minimum gap between two rows of S and $d \leq \frac{1}{3}m$. In fact, by Lemma 5.1, we can deduce the strict inequality $d < \frac{1}{3}m$, since $d = \frac{1}{3}m$ could only be achieved by having nine equally spaced rows.

Let x be a column of S. In each of the following three cases we deduce the existence of a diagonal pair including one entry in column x.

Case 1. $x \in [1, m - 2d - 1] \cup [m, 3m - 2d - 2] \setminus \{2m - 2d - 1, 2m - d - 1, 2m - 1\}$.

By assumption, there is some symbol a such that S includes $(0, x, a)$ in $\mathcal{D}[x]$. Thus S must include the symbol a in row d, which occurs as $(d, x + 2d, a)$ in $\mathcal{D}[x + d]$. This implies that S includes the entry in row 0, column $x + 2d$, which is $(0, x + 2d, a - 2d)$ in $\mathcal{D}[x + 2d]$. Finally, symbol $a - 2d$ in column x must appear in S. Thus S contains

$(-d, x, a-2d)$ in $\mathcal{D}[x+d]$. We therefore have the diagonal pair $(-d, x, a-2d)$ and $(d, x+2d, a)$ in S.

Case 2. $x \in [d+1, m-d-1] \cup [m+d, 3m-d-2] \setminus \{2m-d-1, 2m-1, 2m+d-1\}$.

By similar arguments to Case 1, and using $d < \frac{1}{3}m$, we deduce that S must contain $(0, x, a)$ in $\mathcal{D}[x]$, $(d, x, a+2d)$ in $\mathcal{D}[x-d]$, $(d, x+2d, a)$ in $\mathcal{D}[x+d]$ and $(2d, x+2d, a+2d)$ in $\mathcal{D}[x]$. We therefore have the diagonal pair $(0, x, a)$ and $(2d, x+2d, a+2d)$ in S.

Case 3. $x \in [2d+1, m-1] \cup [m+2d, 3m-2] \setminus \{2m-1, 2m+d-1, 2m+2d-1\}$.

By similar arguments to Case 1 we deduce that S contains $(0, x, a)$ in $\mathcal{D}[x]$, $(d, x, a+2d)$ in $\mathcal{D}[x-d]$, $(0, x-2d, a+2d)$ in $\mathcal{D}[x-2d]$ and $(-d, x-2d, a)$ in $\mathcal{D}[x-d]$. We therefore have the diagonal pair $(-d, x-2d, a)$ and $(d, x, a+2d)$ in S.

We have shown that in each case there is a diagonal pair that includes one entry in column x. We claim that the three cases between them include all integers $x \in [0, 3m-1] \setminus \{0, 2m-1, 3m-1\}$. This follows because $m \geq 3d+1$ implies the inequalities $m-2d \geq d+1$, $m-d \geq 2d+1$, $3m-2d-1 \geq m+d$ and $3m-d-1 \geq m+2d$.

Thus, by Lemma 5.2, the subsquare S may involve at most two columns from $[0, 3m-1] \setminus \{0, 2m-1, 3m-1\}$. The maximum possible number of columns involved in S is therefore five, contradicting the assumption that the order of S is at least nine. □

Acknowledgement

Webb's research was partly supported by an LMS Scheme 4 grant.

References

[1] L.D. Andersen, E. Mendelsohn, A direct construction for Latin squares without proper subsquares, in: Algebraic and Geometric Combinatorics, in: North-Holland Math. Stud., vol. 65, North-Holland, Amsterdam, 1982, pp. 27–53.
[2] J. Dénes, A.D. Keedwell, Latin Squares and their Applications, Akadémiai Kiadó, Budapest, 1974.
[3] J. Dénes, A.D. Keedwell, Latin Squares: New Developments in the Theory and Applications, in: Annals of Discrete Math., vol. 46, North-Holland, Amsterdam, 1991.
[4] R.H.F. Denniston, Remarks on Latin squares with no subsquares of order two, Util. Math. 13 (1978) 299–302.
[5] J.R. Elliott, P.B. Gibbons, The construction of subsquare free Latin squares by simulated annealing, Australas. J. Combin. 5 (1992) 209–228.
[6] B.D. McKay, I.M. Wanless, Most Latin squares have many subsquares, J. Combin. Theory Ser. A 86 (1999) 323–347.
[7] I.M. Wanless, Latin squares with one subsquare, J. Combin. Des. 9 (2001) 128–146.
[8] I.M. Wanless, Diagonally cyclic Latin squares, European J. Combin. 25 (2004) 393–413.